RSAC 2025 Conference

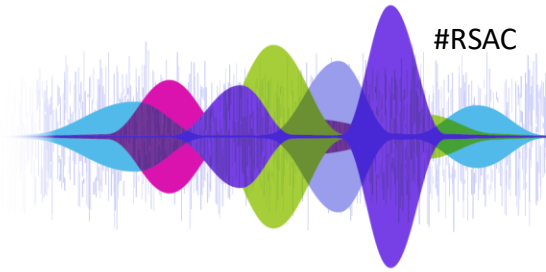
Many Voices.
One Community.

SESSION ID: CTF-W08

Crafting Effective Table-top Exercises for Cybersecurity Leadership

Abhijith “Abx” B R

Founder and Head of Research at BreachSimRange.io
Founder of Adversary Village
in.linkedin.com/in/abhijith-b-r



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Background

- Importance of Table-top exercises
  - Leadership must be prepared for threats, and TTXs provide a structured way to simulate real-world incidents in a controlled environment
  - Many decision-makers are unfamiliar with the complexities of incidents, leading to ineffective responses during critical situations.
- Gaps in coordination
  - Poorly designed table-top exercises lack realism, fail to simulate the pressure of actual incidents
  - Cyber incidents require collaboration across different teams.

Addressing the Incident on the table

Agenda

- Introduction to Table-top exercises
- Learn about cyber threat intel assisted TTXs
- Explore planning and creating TTXs
  - Creating simulated scenarios
  - Planning and execution
  - Post-exercise debrief and analysis
- Wrap-up and lessons learned

RSAC 2025 Conference

Gamified version of a live TTX

Lab 1

Play choose your own TTX adventure

https://ttx.game-URL.TLD

RSAC 2025 Conference

Gathering and analyzing threat-intel

Lab 2

Many Voices.
One Community.

Cyber threat intel to TTX narrative

- Relevant threat intel sources
  - Gather intel on adversaries relevant to the organization
  - Map adversary behaviors to the organization's threat landscape, ensuring the TTX simulates attack scenarios based on actual cyber threats
- Prioritize
  - Prioritize threats based on potential impact on the organization; sector-specific attack trends, previous incidents etc.
- Integrate intel to craft realistic TTX narratives

RSAC 2025 Conference

Identifying threat actors and adversaries

Lab 3

Many Voices.
One Community.

Adversary profiles for TTX

- Realistic organizational threats
  - Align adversary profiles with industry-specific threats and past incidents to simulate realistic stories and scenarios
  - Determine whether the threat actor is financially motivated, state-sponsored, or an insider threat to build scenarios and response strategies

Threat actors and cyber adversaries

Threat actors and cyber adversaries

RSAC 2025 Conference

Creating simulated scenarios for story telling

Lab 4

Many Voices.
One Community.

Crafting Your Story

- Be realistic as possible
  - Craft a scenario that reflects real-world cyber threats, incorporating adversary tactics and potential business impacts to create an immersive experience
  - Use staged decision points to simulate evolving threats, such as data leaks, ransom demands, or regulatory issues, to challenge decision-making
  - Align scenarios with industry-specific risks and realistic organizational challenges, making them actionable for participants

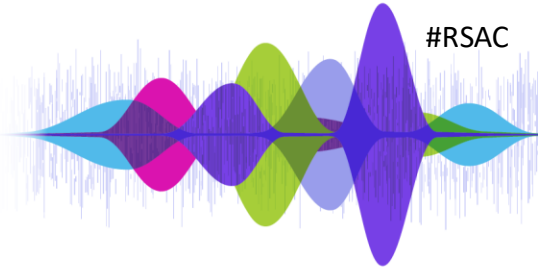
Targeted Ransomware Attack

- Simulated scenario
  - A ransomware group gains initial access to your organization by phishing the cloud system administrator.
  - The threat actor then exfiltrates Personally Identifiable Information (PII) and deploys ransomware on critical servers and endpoints.

TTX Structure

- Incident briefing
- Participant roles
- Incident simulated scenario
  - A ransomware group gains initial access to your organization and deploys ransomware
- Guided discussions with decision points
- Post exercise debrief

Exercise guidelines



- Quick guidelines
  - This exercise is designed to be open in a no-fault environment where diverse perspectives are encouraged
  - Participants should apply their knowledge of existing plans, capabilities, and personal experience to navigate the scenario effectively
  - The exercise is exploratory in nature, decisions made here do not establish formal policies but serve to generate potential solutions, strategies, and actions for addressing cyber threats
  - There are no hidden challenges or trick questions. The provided resources and materials serve as the foundation for discussion.

RSAC 2025 Conference

Planning and execution of the TTX

Lab 5

Many Voices.
One Community.

Overview of creating a practical plan

- TTX name and schedule
- Activities
  - Incident briefing, discussions, simulated decision points, post debrief
- Purpose and objectives
- Scenario and incident
- Compiling the final plan

RSAC 2025 Conference

Execution: Targeted Ransomware

Lab 6

Decision points and questions

- Decision points
  - Initial access has been identified, breach of critical systems and defenses
  - Sensitive data exfiltration, Ransom note for 100K $$
- Questions
  - What indicators help differentiate normal outbound traffic from potentially malicious activity?
  - What backup systems are in place to maintain operations if primary systems are compromised?
  - How are critical systems prioritized and addressed within your incident response plan?
  - Which external partners would you engage for support during a cyber incident?

RSAC 2025 Conference

Post-exercise debrief and analysis

Lab 7

Many Voices.
One Community.

Post TTX

- Facilitate a structured discussion to evaluate decision-making, response effectiveness, and coordination across different teams
- Identify strengths and gaps
  - Document key takeaways, including what worked well and areas needing improvement
- Provide actionable recommendations to enhance incident response plans

Apply What You Have Learned Today

- Next week you should:
  - Identify the threat actor or adversary groups targeting your industry
  - Craft micro scenarios to brainstorm with your team
- In the first three months following this presentation you should:
  - Preparing a TTX execution plan
  - Which is realistic and relevant to your organization
- Within six months you should:
  - Execute a full-fledged Table-top exercise for your Leadership team
  - Identify the gaps and suggest improvements

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You!